WSA New Trusted Root Certificate Bundle Update - April 2017

Inhalt

Einführung

In diesem Dokument werden Details zur Aktualisierung der Cisco Trusted Root Bundles vom April 2017 und deren Auswirkungen auf die Cisco Web Security Appliance (WSA) beschrieben.

Hintergrundinformationen

in dem Bemühen, die Sicherheit unserer Produkte auf höchstem Niveau zu erhalten; Das Cisco Cryptographic Services-Team stellt die nächste Generation der Cisco Trusted Root Bundles vor. Diese Änderung wirkt sich auf die WSA aus. Die Pakete werden automatisch auf allen unterstützten Versionen von Cisco AsyncOS für Web aktualisiert. Die WSA-Administratoren müssen keine Aktionen durchführen.

Beschreibung aktualisieren

Diese Pakete enthalten die neuesten Updates für die Pakete, die ab November 2016 von Upstream-vertrauenswürdigen Root-Stores abgeleitet wurden.

Zu beachten sind die wichtigsten Änderungen an Cisco Trusted Root Bundles:

- Aufgrund der Entscheidung großer Vertrauensbanken (Google, Apple, Mozilla), diese zu entfernen, enthalten die neuen vertrauenswürdigen Cisco Root-Pakete keine Wurzeln mehr von WoSign/StartCom. Wenn sie neue Stammverzeichnisse in Upstream-Root-Stores einsenden, werden wir die Entscheidung, diese aus den Trust-Paketen zu entfernen, erneut überprüfen.
- Die neue Cisco Root CA 2099 wurde zu allen Paketen hinzugefügt, um neue ACT2-Chipsätze zu unterstützen.
- Der alte VeriSign-Root wurde im Core-Paket durch den neueren Root ersetzt, der VeriSign-mPKI-Zertifikate korrekt ketten soll.
- Die DST Root CA X1 wurde nur aus dem Core-Paket entfernt, da Cisco keine Wurzeln mehr aus dieser Kette wirft.

Was bedeutet dies für WSA-Benutzer?

- Die Cisco WSA lädt neue Stammzertifikatpakete herunter, die unseren Aktualisierungsvorgang nutzen. WSA-Administratoren müssen keine Maßnahmen ergreifen.
- Wenn die WSA so konfiguriert ist, dass sie die Entschlüsselung verwendet, werden Anfragen an Sites, die über SSL-Zertifikate verfügen, die von **WoSign/StartCom** signiert wurden, standardmäßig von der WSA verworfen, da die Zertifikate der Root-Zertifizierungsstelle dieses Anbieters nach der Aktualisierung nicht von der WSA vertrauenswürdig sind.
- Alternativ kann die WSA die in **HTTPS-Proxy** konfigurierte Aktion **> Invalid Certificate Handling > Unknown Root Authority/Issuer** anwenden. Diese Aktion ist standardmäßig DROP, und Cisco empfiehlt, die Standardaktion für nicht erkannte Root Authority nicht zu ändern.